Governmental Cloud Security Problems

ROUMEN TRIFONOV
Faculty of Computer Systems and Control
Technical University of Sofia
8 st. Kliment Ohridski bul., 1000 Sofia
BULGARIA
r_trifonov@tu-sofia.bg

Abstract: - There are no guidelines to define a generic security framework that allows assessing and benchmarking Governmental Cloud security and the proper problems. The recent European studies testify that so far is no comprehensive analysis of the security frameworks of currently running or planned governmental Cloud deployments. The present article aims to outline the security problems and some key points for building Governmental Cloud Security Framework including Risk Assessment, Security Measures, Service Level Agreement, Security Certification and Incident Reporting.

Key-Words: - Governmental cloud, risk assessment, security measures, service level agreement, security certification, incident reporting

1 Introduction

The idea of a central or local government leveraging the Cloud computing business model to increase the effectiveness and efficiencies of the ICT services is appealing, especially in a period of economic challenges for the European Union Member States. The concept of Governmental Cloud (Gov Cloud) proposes, among others, the following [1]: "*…Cloud computing service delivery model satisfies the most of the needs of public aministrations, on the one hand, since it offers scalability, elasticity, high performance, resilience and security. However, many public bodies have not yet built a model for assessing their organizational risks related to security and resilience."*

A standard definition for the term Gov Cloud is currently lacking. However, we can adopt the Gov Cloud definition introduced by ENISA report [2], as:

"- *a Gov Cloud is an environment running services compliant with governmental and EU legislations on security, privacy and resilience (what);*

- *a Gov Cloud is a secure and trustworthy way (private Cloud or public Cloud) to run services under public body governance (how);*

- *a Gov Cloud is a deployment model to build and deliver services to state agencies (internal delivery of services), to citizens and to enterprises (external delivery of services to society) (for who)."*

One of the main features of the GovCloud is that it implements e-Government functions of delivery of administrative services, i.e. the functions of the user and the service provider(s) are distinguished (Fig. 1).

The compelling business and financial benefits for adopting Cloud services require formalization of a security framework for governmental clouds. This security framework can be based on a collection and analysis of existing Cloud computing security literature, other relevant security best practices, and on the few existing real life case studies of Governmental Clouds in Europe.

In principle the security framework is as a conceptual structure intended to serve creation of a secure information system. In our case, the intention of the security framework is to serve as a comprehensive guideline for the creation, deployment, assessment and improvement of a secure Gov Cloud. It should be considered as the beginning of a continuous enhancement process by incorporating emerging elements, and by considering the lessons learned from its real-world application.

The new European Information Security Directive [3] states that the Cloud computing services span a wide range of activities that can be delivered according to different models.

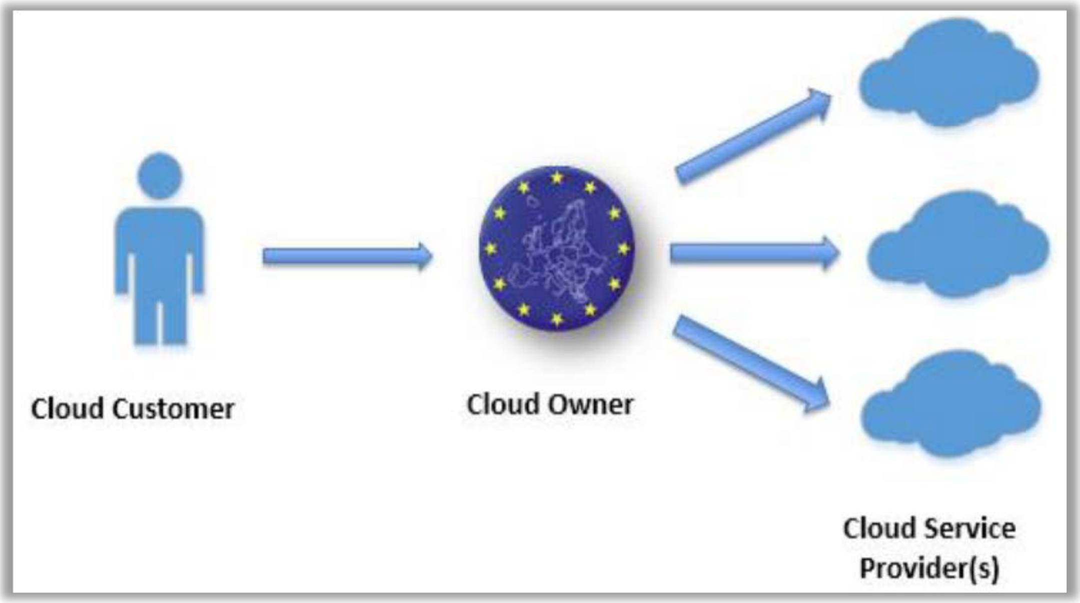

Fig. 1 GovCloud

In this regard, the Directive introduces the following terms: the term "cloud computing services" covers services that allow access to a scalable and elastic pool of shareable computing resources. Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services. The term "scalable" refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term "elastic pool" is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term "shareable" is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment.

The European study of Governmental Cloud Security Framework [4] concluded that:

- security and privacy issues are considered as key factors to take into account for migration, and at the same time are the main barriers for adoption. Protection of sensitive data is still an issue seeking solution, spanning from the Service Level Agreement (SLA) provisions to the actual technological mechanisms i.e. encryption etc.;

- there is a clear need for Cloud pilots and prototypes in order to test the utility of the technology. There is also a need for best practices and success stories to be disseminated in the EU public administration community;

- the main security challenges, requirements and barriers in the cloudification of governmental services are related to: data protection and compliance, interoperability and data portability, identity and access management, auditing, adaptability and availability, as well as risk management and detailed security SLA formalization;

- there are no current studies that comprehensively analyse the security frameworks of currently running or planned governmental Cloud deployments. Hence, there are no guidelines to define a generic security framework that allows to assess and benchmark Gov Cloud security.

In these circumstances, the present article aims to outline some key points for building Governmental Cloud Security Framework.

2 Risk Assessment for Cloud

It is necessary to find a pragmatic approach for assessing risks to Cloud applications (cloud SaaS applications) and applications hosted in Cloud environment (applications using cloud based IaaS and PaaS). This can be done by developing methods for assessing the impact level of breaches and then try to define a methodology for mapping the impact levels on required technical and organizational measures and certifications.

A full risk analysis using classical methods can be very time consuming and might make sense for high-profile (expensive) applications. It is advisable to use simpler risk assessment and simple tools to identify the necessary protection measures and controls.

The threats related to the security of the cloud hosting environment and infrastructure layer can be covered by the certification of the underlying IaaS layer. Since the likelihood may depend on the implemented security controls and protection or redundancy mechanisms, it is important to document the assumptions under which this likelihood is valid. For Governmental Cloud applications the entire attacker community, including organized crime and state sponsored espionages, are important threat agents. In Cloud computing environment for applications with high value or high loss potential it is safe to assume that threat agent's capabilities are very high.

That's why, the methods which determine which measures and controls need to be implemented depend on the impact assessment of the elements of cloud technologies (SaaS, PaaS, IaaS). The applications and the way it use must be analysed in order to guarantee security and to avoid lock-in.

The article [5] defines the risks specific to government use of cloud computing, wish contain various forms of risk associated with cloud computing, and highlight key elements essential for any risk management plan intending to identify, manage and mitigate these risks:

2.1 Tangible/known risks

2.1.1 Access

An organization's private data must be secured to ensure that only authenticated users are allowed the access authorized by the customer – the governmental agency, in this case–and that any unwanted or outside access requests are denied. This shared physical server model requires the vendor to ensure that each separate customer's data remains segregated so that no data bleeding occurs across virtual servers. To further complicate the issue, a single file or data storage area may be distributed among multiple physical servers over several states; this may distribute the risk of a single point of failure, but creates multiple possible points for intrusion. In administrative information processing, requirements to comply with governmental privacy and information integrity laws are common for traditional enterprise systems but are not explicitly defined for the Cloud. The Cloud infrastructure must also provide the required logging, tracking, and monitoring capabilities that would be commonly found on an internal server.

2.1.2 Availability

A key selling point to Cloud computing has been the potential for 100%, non-interrupted availability to the customer. Natural disasters and other unexpected events can cause Cloud services to become unavailable. Another risk to availability is how the priority of users on the Cloud is determined should the overcapacity threshold is reached.

2.1.3 Infrastructure

The underlying Cloud infrastructure and environment must be designed and implemented to be flexible and scalable. If not implemented properly, the government risks significant challenges and costs in migrating information to different technologies as the third-party vendor upgrades its processing and storage environment. If this type of upgrade is managed in-house, resident IT professionals can more readily manage migration and harmonization of data, users, and processes. But the procedures that a cloud vendor executes in scaling its environment is managed without the input of its customers, and may change or nullify the services the customer requires.

2.1.4 Integrity

Any information housed within a Cloud infrastructure must maintain its integrity–its accuracy within its context–to be of value to the customer. The Cloud provider must ensure that all precautions are taken to guarantee that data within the cloud storage does not become corrupt or altered; this is not a safe assumption without a defined Service Level Agreement. Due to a lack of governmental policy and a dearth of challenging case law, who owns information (and its metadata and forensics) once it is remanded to a cloud's custody is not clear.

2.2 Intangible/unknown risks

There are many law and policy issues raised by Cloud computing that could become problematic for governmental agencies, both as Cloud users and as Cloud providers. Given the relatively undeveloped and unproven state of governmental Cloud policies and the widespread unknowns that weave into the question of whether the administration can successfully identify and manage the risks of working in a Cloud environment, proceeding with caution until policies, standards, and technical proficiency are addressed will help the government avoid any unwanted risks.

The study [6] draws attention to another risk associated with the vulnerability in virtualization. The virtualization is one of the main components of a Cloud. But this poses major security risks. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization, which is not met completely in today’s scenario. The other issue is the control of administrator on host and guest operating systems. Some vulnerability has been found in all virtualization software which can be exploited by malicious, local users to bypass certain security restrictions or gain privileges. For example, the vulnerability of Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system. Vulnerability in Virtual PC and Virtual Server could allow elevation of privilege.

In March 2010, the Cloud Security Alliance (CSA) published a document [7], which includes the top seven threats as identified by its members. More recently, in April 2011, the Open Web Application Security Project (OWASP) released a ‘pre-alpha list’ of its top 10 cloud security risks derived from a literature review of other publications and sources [8]. In May 2011, the National Institute of Standards and Technology (NIST) released new Special Publication [9], which provides a deep analysis of risk. In July 2011, ISACA released an issue [10], which provides a comprehensive guide to cloud controls taken from COBIT, Val IT and Risk IT. This publication highlights both the need for a consistent and broadly accepted risk assessment framework and the fact that its existence still remains elusive.

One of advisable methods for risk assessment in Govenmental Cloud applications can be so called “Risk-based Security Assessment and Testing Methologies” defined in the Guide EG 203 351 of European Telecommunication Standardization Institute (ETSI) [11]. This guide introduces test-based risk assessment, which is able to verify the assumption on risk factors with tangible measurement and test results.

In general, the testing activities (Fig. 2) can be divided into functional security testing, robustness testing, performance testing and penetration testing.

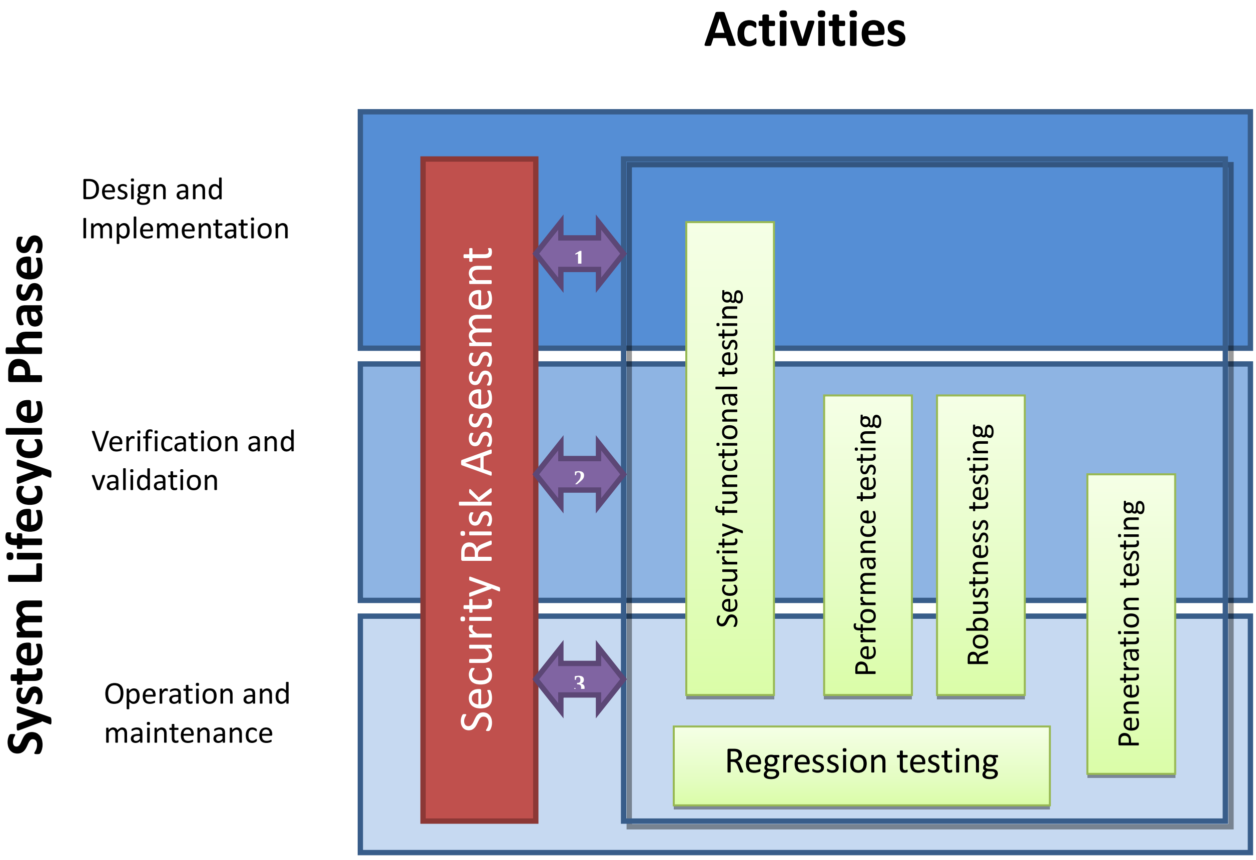

Fig. 2 The Testing Activities according to the Guide 203 351

While functional security testing, robustness testing and performance testing are used to check the functionality, availability and efficiencyy of the specified security functionality and systems (e.g. firewalls, authentication and authorization subsystems access control), penetration testing (or security vulnerability testing) directly addresses the identification and discovery of so far undiscovered system vulnerabilities caused by security design flaws.

3 Security Measures

The European study [12] recommends to governments to adopt a staged approach, with the ability of backtracking each stage, because the complexity of the Cloud environment introduces a number of unknown variables that could be very difficult to manage. The administrations at any level should consider system interconnection and interdependencies (most of which may be unknown), especially when simultaneously moving multiple services to a Cloud system(s). They should consider this caveat in the context of a dynamically changing environment and a currently incomplete understanding of vulnerability and attack mechanisms, and the complexity of related controls. The administrative bodies should not assume that the successful deployment of an application in a Cloud environment is automatically a positive indication for proceeding with many other deployments; the security and resilience requirements of each application should be examined carefully and individually and compared to the available Cloud architectures and security controls.

Guided by these recommendations, the author has selected some security measures, which are the most adequate to the recommended approach:

3.1. Loss of control of data and resources is one of the main barriers to Gov Cloud take-up. The “loss of control” issue is not only a matter of technologies but also of awareness, transparency, regulation, contractual agreements between providers and governmental customers. Another aspect of “loss of control” is the vendor lock-in problem i.e. what is the mitigation action for bankruptcy of the Cloud provider cases. Concerning vendor lock-in, from a technical point of view, without cost and time constraints, it should always be possible to migrate data and applications from one Cloud provider to another.

The competent authorities in cooperation with Cloud providers and government customers should closely work to mitigate “loss of control” addressing the issues of governance, monitoring and auditing, vendor lock-in and data handling. Required steps are:

- definition of a monitoring framework for Gov Cloud public service layers;
- definition of standard procedures for data handling;
- definition of standard procedures for data and service migration.

3.2. Cloud providers usually store data in their datacentres which can be located in many different places. The possibility to locate data and resources is often perceived as a barrier for Gov Cloud adoption rather than an advantage for data privacy issues. The definition of regulatory framework for data location can reduce the risks of objections from the governmental users, but the most critical concern for data protection is to ensure the security of data more than location of data.

To achieve this, it is necessary that the competent authorities in cooperation with Cloud providers and government customers could work closely on the following topics:

- definition of measures to improve the awareness of government agencies and Cloud service providers on existing EU legislation on the subject;
- foster the development of technological solutions compliant with the existing legislation;
- categorization of specific governmental institution requirements on data ownership and data privacy judged by the type of data handled;
- enhancement of the existing legislation on data and resource ownership with a focus outsourcing;
- enhancement of the existing legislation on data privacy with a focus on outsourcing.

3.3. The public users and providers should be free to choose the level of security provided and requested for the public services, with positive effects on the competition between providers and leaving the departments the possibility for implement the most effective and the best value for money solutions. A specific set of security measures focussed on Governmental Cloud deployment would be the way to improve trustworthiness in the Cloud supply chain. Suggested actions to enhance the security and protection of information for the Governmental Cloud services are:

- support pre-assessment process before procuring services;
- create a set of baseline security measures focussed on Governmental Clouds; for this reason

the measures should include domains like security management, identity management, data redundancy, services availability etc;

- include risk impact levels in each domain in order to offer a sohpistication/maturity model;
- enable voluntary auditing (and/or certification) framework of information security measures;
- foster security labelling systems.

4 The Service Level Agreement as a Factor for Cloud Computing Security

The study [13] raises the question about the role of the Service Level Agreement in Cloud computing.

Usually, a third party could be used to monitor the data or the whole system that comes in between of the provider and customer. This third party works with the service provider and client to control and save the Data Centre. In Cloud computing, the Private Virtual Infrastructure (PVI) model has been suggested to distribute the responsibility of control and save the Data Centre between providers and clients. In this model, users have security over their information in the cloud, and providers would have security over the fabric of the server.

Service level agreement (SLA) between client and provider is critical to defining the roles and responsibilities of all parties involved in using and providing cloud services. The SLA should explicitly call out what security services the provider guarantees and what the client is responsible for providing.

Under these circumstances the Model of Cloud SLA Assurance Methodology (Fig. 3) must be developed in order to formulate the main factors of having secure data agreement in Cloud computing.

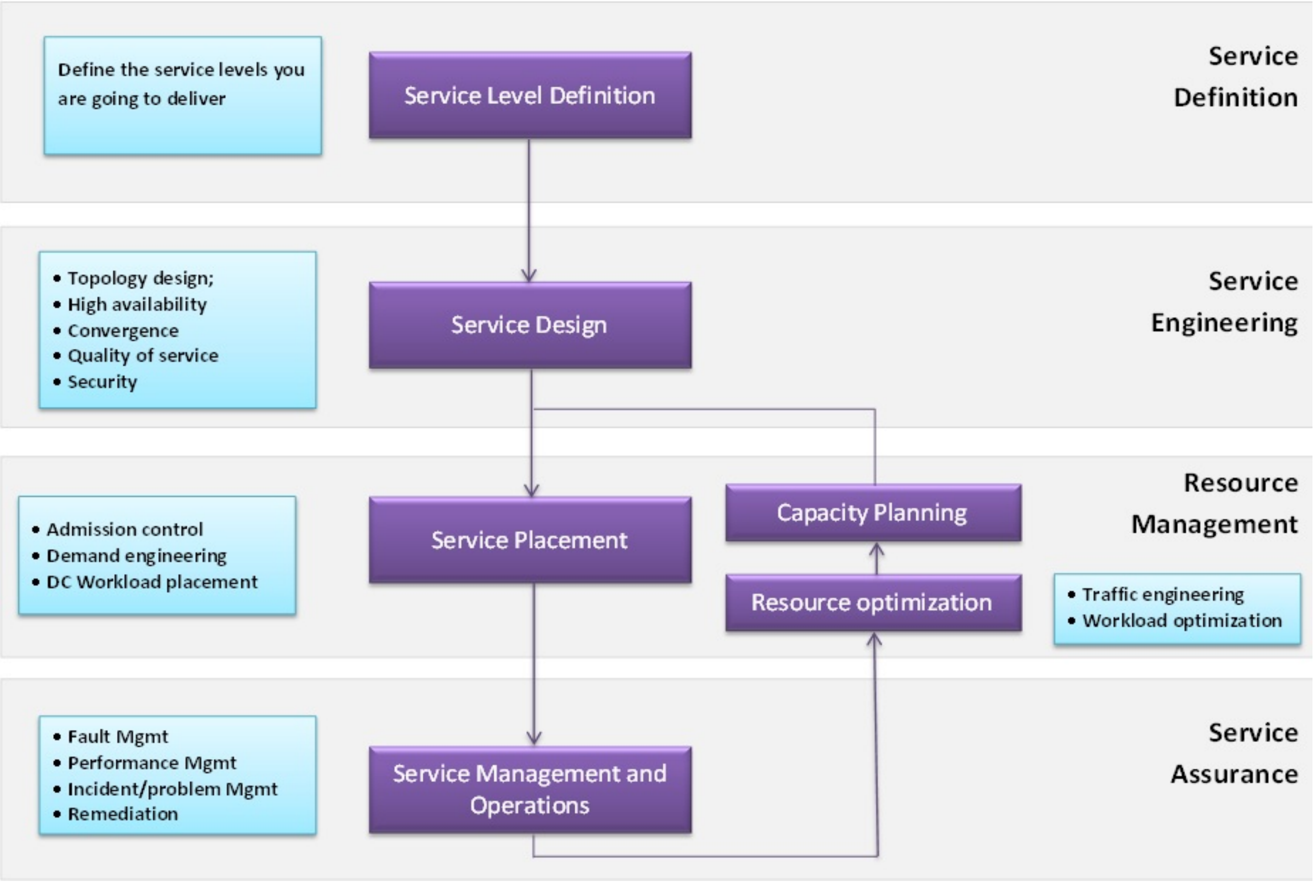

Fig. 3 Cloud SLA Assurance Methodology

Usually, services providers don’t explain the geographical location of the servers. So, many customers don’t trust these services from that provider. Consequently, different governmental agencies might ask the provider to locate their data in boarder of the country or in specific location that they trust to avoid the hacking or losing the data. SLA helps to manage this factor by state the conditions that the provider and the consumer must follow and the penalties that they might get in case of breaking these conditions.

One of main factors that the consumer of Cloud computing should know is the how long of time that his data be available in cloud [15]. In the other words, when and how has the ability to delete or move the data from the servers. SLA could help to manage this factor. In general, the consumer has the rights to manage the data via the third party, so managing the period of time or moving and deleting the data is one of the consumers job. However, the trust is playing a main role here. The impact and destruction for resources in Cloud computing is worse than the current real Internet environment which also shares the recourses. Therefore, whether or not the behaviour of the cloud users are trusted, the question still exist which is how can evaluate the user behaviour in trustworthy point of view. The process of evaluating the trust can be one of the major items in such Cloud SLA Assurance Methodology Model.

In Cloud computing environment, verifying security happens by leading every service to be able to report security facilities in present and verify it. So, these ability means the client needs to have the authority to configure and set this matter. Therefore, the use of above mentioned Model can make the negotiation between the customers and providers more equitable, convenient and transparent.

5 Cloud Security Certification Framework

In general, the Cloud Security Certification is a part of so called “Cloud Computing Certification Schemes (CCCS)”, which include also certification procedures for Interoperability, Service Management, Reliable Access and Privacy/Data Protection.

Currently, there are 24 internationally recognized certification schemes in the field of information security. The classic scheme based on ISO/IEC 27001/27002 is hardly suitable for cloud application because of the orientation of these standards for needs of consolidated organization. In our opinion for information security certification of the Gov Cloud can be recommended so called “EuroCloud Star Audit (ECSA)” [5]. This is a certification scheme especially designed to assess “on-line” services. It evaluates an “on-line” Cloud service against the requirements of audit scheme and covers all participants of the specific supply chain of a service. The ESCA audit is a not-negotiable mandatory bandwidth of all important areas: provider’s profile, contract and compliance including data privacy protection against local law, security, operations, environment and technical infrastructure, processes and relevant parts of the application and implementation up to interoperability and data portability.

6 Cloud Security Incident Reporting

The Governmental Cloud computing probably will become the backbone of e-Government applications. That’s why certain Cloud security incidents could have a major impact in society and the incident reporting about Cloud security incidents could be implemented in an effective and efficient way.

The expert’s perspective on the key issues of Cloud security incident reporting can be summarized as follows:

- it is difficult to assess the criticality of the Cloud services for a national regulator. There are many interdependencies, different layers of the cloud stack, different deployment models and different kind of data stored;

- Cloud services are often based on other Cloud services; they are distributed systems and built up in several layers. Incident reporting is different in these different layers;

- from the Cloud customer’s point of view, most standard contracts do not commit providers to reporting about security incidents to customers. Even though, some Cloud providers do have dashboards where some incidents are published and explained;

- from the provider’s side, it is up to the customer to include incident reporting obligations in contracts. For this reason, in many Cloud contracts incident reporting is not addressed;

- incident reporting is becoming more and more common in regulated sectors, like governmental administration where operators need to report incidents to regulators;

- incident reporting should be part of a bi-directional flow of information where providers report about security incidents to authorities and authorities’ feedback common threats and common issues to the Cloud providers so they can improve security and resilience.

If the Cloud provider offers IaaS/ PaaS/ SaaS services to administrative bodies, he has signed a contract with the administrative institutions. When an incident happens, impacting the availability of the core systems of the customers, the provider will send, according to the contractual terms, a report with the technical specifications, the causes and remediation actions including impact analysis to the customer.

In the case of overruns certain threshold of impact (regulated by the national regulatory authority), the operator must report to this authority, since it is the one that collects more information on the scale of the impact (and is aware of the criticality of the services and data processed).

4 Conclusion

Having in mind the strong opinion about the prospects of Cloud applications as the basis for Electronic Governance in Europe and also, the documented intentions of the Bulgarian government to create National Governmental Cloud, this article aims to outline the problems related to the Governmental Cloud network and information security.

The article recommends possible approaches and solutions to these problems, based on the good European and international practices.

References:

[1] Unleashing the Potential of Cloud Computing in Europe Communication from the European Commission (2012) 529 final

[2] Good Practice Guide for securely deploying Governmental Clouds ENISA 2013

[3] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[4] Security Framework for Governmental Clouds ENISA 2015

[5] Scott Paquette, Paul T. Jaeger, Susan C. Wilson Identifying the security risks associated with governmental use of cloud computing *Government Information Quarterly* No 27 Elsevier (2010) 245 - 253

[6] S. Subashini, V. Kavitha A survey on security issues in service delivery models of cloud computing *Journal of Network and Computer Applications* No 34 Elsevier (2011) 1 – 11

[7] Top Threats to Cloud Computing V1.0, Cloud Security Alliance, 2010, www.cloudsecurityalliance.org/Topthreats

[8] OWASP Cloud—10 Project, OWASP, 2011, www.owasp.org/index.php/Category:OWASP_Cloud_ _10_Project

[9] Cloud Computing Synopsis and Recommendations *Special Publication* 800-146, NIST, 2012

[10] IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, ISACA, 2011, www.isaca.org/cloud

[11] Methods for Testing & Specification; Risk-based Security Assessment and Testing Methodologies ETSI EG 203 251, 2015

[12] Security and Resilience in Governmental Cloud ENISA 2011

[13] Hamoud Alshammari, Christian Bach Administration Security Issues in Cloud computing *International Journal of Information Technology Convergence and Services* (IJITCS) Vol.3, No.4, August 2013

[14] https://staraudit.org

[15] Ljubomir Lazic and Nikos Mastoralis, Cost effective software, test metrics. WSEAS Transactions on Computers Issue 6, Volume 7, June 2008, pp 599-619